Fig. 1

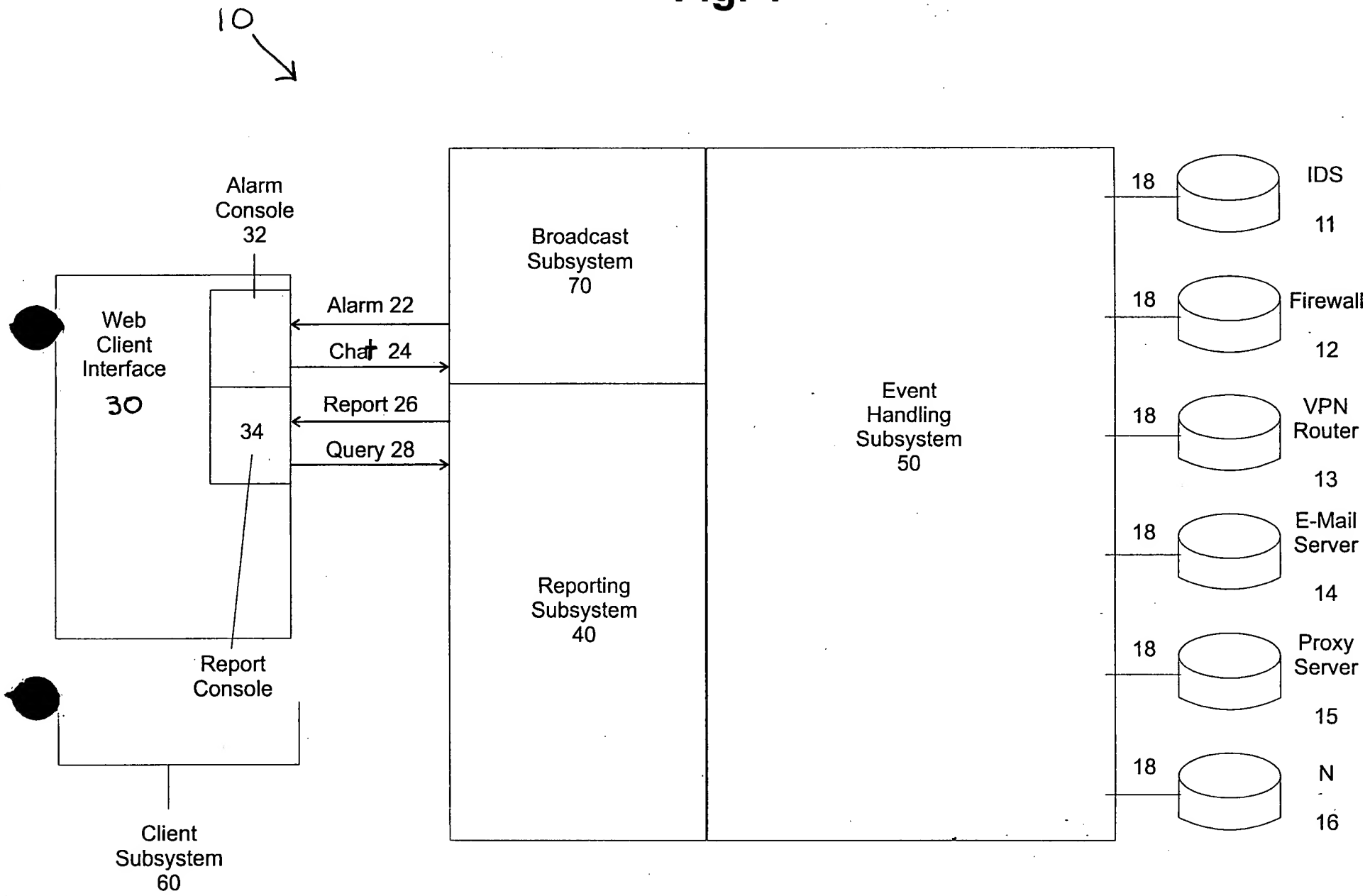
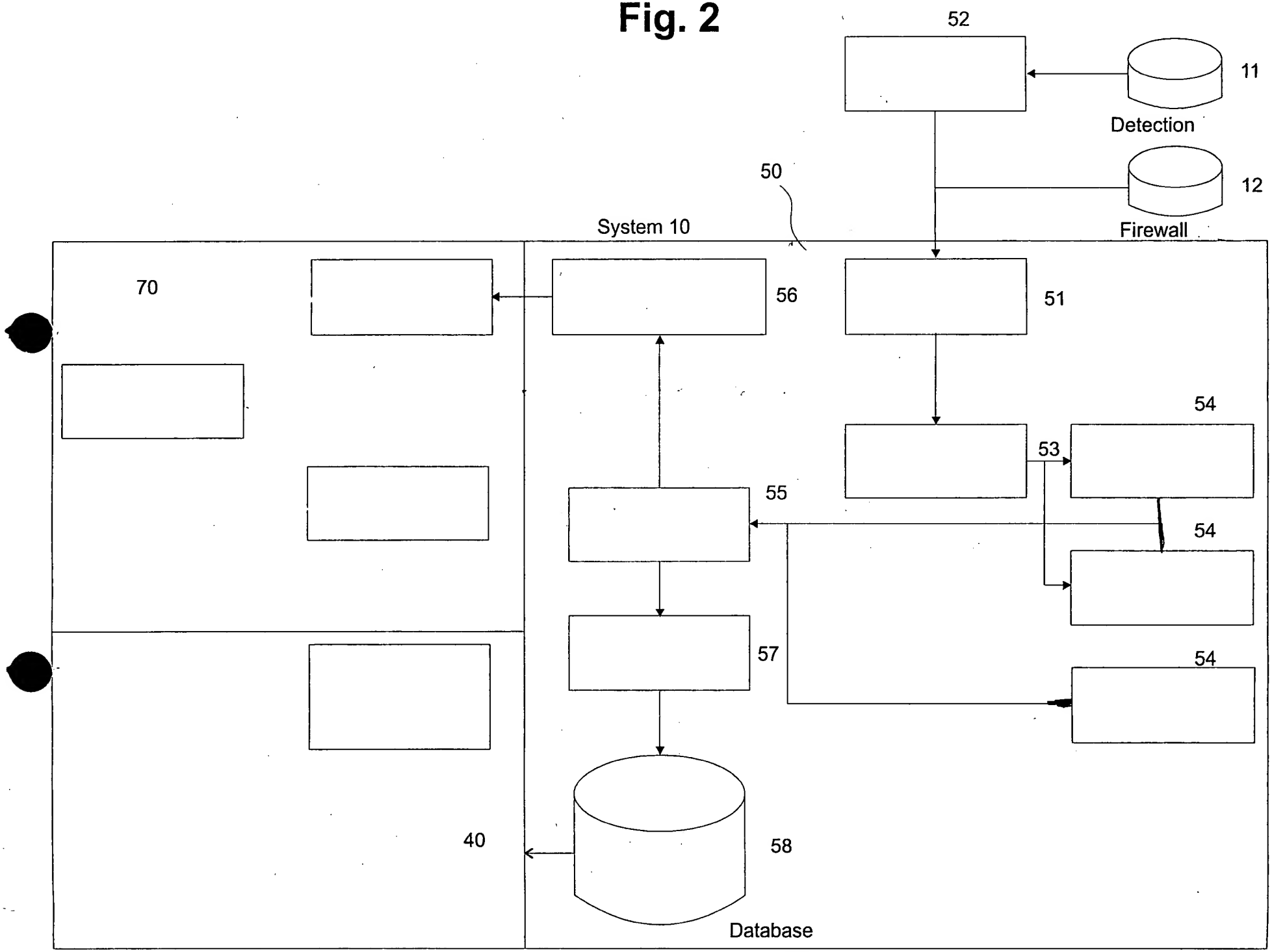

10
Alarm Console 32
Web Client Interface 30
34
Report Console
Client Subsystem 60
Alarm 22
Chat 24
Report 26
Query 28
Broadcast Subsystem 70
Reporting Subsystem 40
Event Handling Subsystem 50
18
IDS 11
Firewall 12
VPN Router 13
E-Mail Server 14
Proxy Server 15
N 16

Fig. 2


52
11
Detection
50
12
Firewall
System 10
70
56
51
54
53
55
54
57
54
40
58
Database

Alert Messages, Severity 1

The following messages appear at severity 1, alerts:

%PIX-1-101001: (Primary) failover cable OK.
%PIX-1-101002: (Primary) Bad failover cable.
%PIX-1-101003: (Primary) failover cable not connected (this unit).
%PIX-1-101004: (Primary) failover cable not connected (other unit).
%PIX-1-101005: (Primary) Error reading failover cable status.
%PIX-1-102001: (Primary) Power failure/System reload other side.
%PIX-1-103001: (Primary) No response from other firewall.
%PIX-1-103002: (Primary) Other firewall network interface chars OK.
%PIX-1-103003: (Primary) Other firewall network interface chars failed.
%PIX-1-103004: (Primary) Other firewall reports this firewall failed.
%PIX-1-103005: (Primary) Other firewall reporting failure.
%PIX-1-104001: Secondary: Switching to ACTIVE (cause: chars).
%PIX-1-104002: (Primary) Switching to STNDBY.
%PIX-1-104003: (Primary) Switching to FAILED.
%PIX-1-104004: (Primary) Switching to OK.
%PIX-1-105001: Disabling failover.
%PIX-1-105002: Enabling failover.
%PIX-1-105003: Monitoring on interface dec waiting.
%PIX-1-105004: Monitoring on interface dec normal.
%PIX-1-105005: Lost failover communications with mate on interface dec.
%PIX-1-105006: Link status 'Up' on interface dec.
%PIX-1-105007: Link status 'Down' on interface dec.
%PIX-1-105008: Testing interface dec.
%PIX-1-105009: Testing interface dec chars.
%PIX-1-105020: (chars) Incomplete/slow config replication
%PIX-1-302001: Built TCP connection for faddr IP_addr/port gaddr IP_addr/port laddr IP_addr/port (chars)
%PIX-1-709003: (chars) Beginning configuration replication: Send to mate.
%PIX-1-709004: (chars) End Configuration Replication (ACT)
%PIX-1-709005: (chars) Beginning configuration replication:Receiving from mate.

Critical Messages, Severity 2

The following messages appear at severity 2, critical:

%PIX-2-106001: Inbound TCP connection denied from IP_addr/port to IP_addr/port flags chars
%PIX-2-106002: TCP Connection denied by outbound list dec src IP_addr/port dest IP_addr/port
%PIX-2-106003: Connection denied src IP_addr dest IP_addr due to JAVA Applet.
%PIX-2-106006: Deny inbound UDP from IP_addr/port to IP_addr/port
%PIX-2-106007: Deny inbound UDP from IP_addr/port to IP_addr/port due to DNS query/response.
%PIX-2-106008: Translation for IP_addr denied by outbound dec
%PIX-2-106009: Translation for IP_addr to IP_addr denied by outbound dec
%PIX-2-106012: Deny IP from IP_addr to IP_addr, IP options hex.
%PIX-2-106013: Dropping echo request from IP_addr to PAT address IP_Addr
%PIX-2-106014: Deny inbound icmp src interface name: IP_addr dst interface name: IP_addr (type dec, code
dec)
%PIX-2-106015: Deny TCP (no connection) from IP_addr/port to IP_addr/port flags.
%PIX-2-106016: Deny IP spoof from IP_addr to IP_addr, IP options hex.
%PIX-2-106017: Packet contains ActiveX content and has been modified src IP_addr dest to IP_addr, IP options
hex.
%PIX-2-108001: SMTP made noop: out chars in chars data: chars
%PIX-2-108002: SMTP replaced chars: out chars in chars data: chars
%PIX-2-109009: Authorization denied from IP_addr/port to IP_addr/port (not authenticated)
%PIX-2-109011: Authen Session Start: user 'user', sid session_num
%PIX-2-110003: No interface is configured (with chars).
%PIX-2-112001: (chars:dec) PIX clear finished.
%PIX-2-199004: PIX clear config char from char.
%PIX-2-201003: Embryonic limit exceeded dec/dec for IP_addr/port (IP_addr)IP_addr/port .
%PIX-2-304006: URL Server went OFFLINE

Figure 3a

Error Messages, Severity 3

The following messages appear at severity 3, errors:

%PIX-3-105010: host failover message block alloc failed
%PIX-3-106010: Deny inbound from outside:IP_addr to inside:IP_addr chars.
%PIX-3-109010: Auth from IP_addr/port to IP_addr/port failed (too many pending auths)
%PIX-3-109013: User must authenticate before using this service
%PIX-3-110002: No ARP for host IP_addr
%PIX-3-201001: Out of connections! dec/dec.
%PIX-3-201002: Too many connections on static IP_addr
%PIX-3-201005: FTP data connection failed for IP_addr.
%PIX-3-201006: RCMD back connection failed for IP_addr/port.
%PIX-3-201007: Unable to allocate new UDP connections (IP_addr/port-IP_addr/port)
%PIX-3-201008: The PIX is disallowing new connections.
%PIX-3-202001: Out of address translation slots!
%PIX-3-202002: Unable to find translation for incoming IP_addr.
%PIX-3-202002: Unable to find translation for SRC=IP_addr DEST=IP_addr IP octal inside|outside.
%PIX-3-202003: Could not build translation for IP_addr.
%PIX-3-202004: Could not build portmap translation for IP_addr.
%PIX-3-203001: ESP Error: No Key SPI hex SRC IP_addr DEST IP_addr
%PIX-3-208005: (chars:dec) pix clear return dec
%PIX-3-304003: URL Server IP_addr timed out URL string
%PIX-3-304004: URL Server IP_addr request failed URL chars
%PIX-3-304006: URL Server IP_addr not responding, trying IP_addr
%PIX-3-304007: URL Server IP_addr not responding, ENTERING ALLOW mode
%PIX-3-304008: Leaving ALLOW mode, URL Server IP_addr
%PIX-3-305005: No translation group found for protocol

Warning Messages, Severity 4

Currently, PIX Firewall does not generate severity 4, warning, Syslog messages.

Notification Messages, Severity 5

The following messages appear at severity 5, notifications:

%PIX-5-109012: Authen Session End: user 'user', sid session_num, elapsed num_seconds seconds
%PIX-5-111001: Begin configuration: chars writing to chars
%PIX-5-111002: Begin configuration: source reading from device
%PIX-5-111003: chars erase configuration
%PIX-5-111004: chars end configuration: FAILED|OK
%PIX-5-111005: chars end configuration: OK
%PIX-5-111006: Console login from chars at chars
%PIX-5-111007: Begin configuration: chars reading from chars.
%PIX-5-111008: User 'chars' executed the 'chars' command.
%PIX-5-199001: PIX reload command executed from IP_addr.
%PIX-5-304002: Access denied URL chars SRC IP_addr DEST IP_addr: chars

Figure 3b

Informational Messages, Severity 6

The following messages appear at severity 6, informational:

%PIX-6-109001: Auth start for user 'chars' from IP_addr/port to IP_addr/port
%PIX-6-109002: Auth from IP_addr/port to IP_addr/port failed (server IP_addr failed)
%PIX-6-109003: Auth from IP_addr/port to IP_addr failed (server IP_addr failed)
%PIX-6-109005: Authentication succeeded for user 'chars' from IP_addr/port to IP_addr/port.
%PIX-6-109006: Authentication failed for user 'chars' from IP_addr/port to IP_addr/port.
%PIX-6-109007: Authorization permitted for user 'chars' from IP_addr/port to IP_addr/port.
%PIX-6-109008: Authorization denied for user 'chars' from IP_addr/port to IP_addr/port.

%PIX-6-302003: Built H245 connection for faddr IP_addr laddr IP_addr/port
%PIX-6-302004: Preallocate H323 UDP backconnection for faddr IP_addr to laddr IP_addr/port
%PIX-6-302005: Built UDP connection for faddr IP_addr/port gaddr IP_addr/port laddr IP_addr/port
%PIX-6-302006: Teardown UDP connection for faddr IP_addr/port gaddr IP_addr/port laddr IP_addr/port duration
time bytes dec (chars)
%PIX-6-302009: Rebuilt TCP connection %d for faddr IP_addr/ port gaddr IP_addr/ port laddr IP_addr/ port
%PIX-6-303002: IP_addr retrieved IP_addr:chars
%PIX-6-304001: IP_addr accessed IP_addr:chars.
%PIX-6-305001: Portmapped translation built for gaddr IP_addr/port laddr IP_addr/port (chars)
%PIX-6-305002: Translation built for gaddr IP_addr to IP_addr
%PIX-6-305003: Teardown translation for IP_addr (IP_addr)
%PIX-6-305004: Teardown portmap translation for global IP_addr/port local IP_addr/port
%PIX-6-305007: Orphan IP IP_addr on interface dec
%PIX-6-307001: Denied Telnet login session from IP_addr.
%PIX-6-307002: Permitted Telnet login session from IP_addr.
%PIX-6-307003: Telnet login session failed from IP_addr (3 attempts).
%PIX-6-308001: PIX console enable password incorrect for 3 tries from IP_addr.
%PIX-6-309001: Denied manager connection from IP_addr.
%PIX-6-309002: Permitted manager connection from IP_addr.

Debugging Messages, Severity 7

The following messages appear at severity 7, debugging:

%PIX-7-106011: Deny self route chars
%PIX-7-304005: URL Server IP_addr request pending URL chars
%PIX-7-305006: type translation creation failed for protocol
%PIX-7-701001: alloc_user() out of Tcp_user objects
%PIX-7-709001: (chars) Rep CI ioctl (chars) return chars
%PIX-7-709002: (chars) Rep no replication chars
%PIX-7-709006: (chars) End Configuration Replication (STB)

Figure 3c

Fig. 4

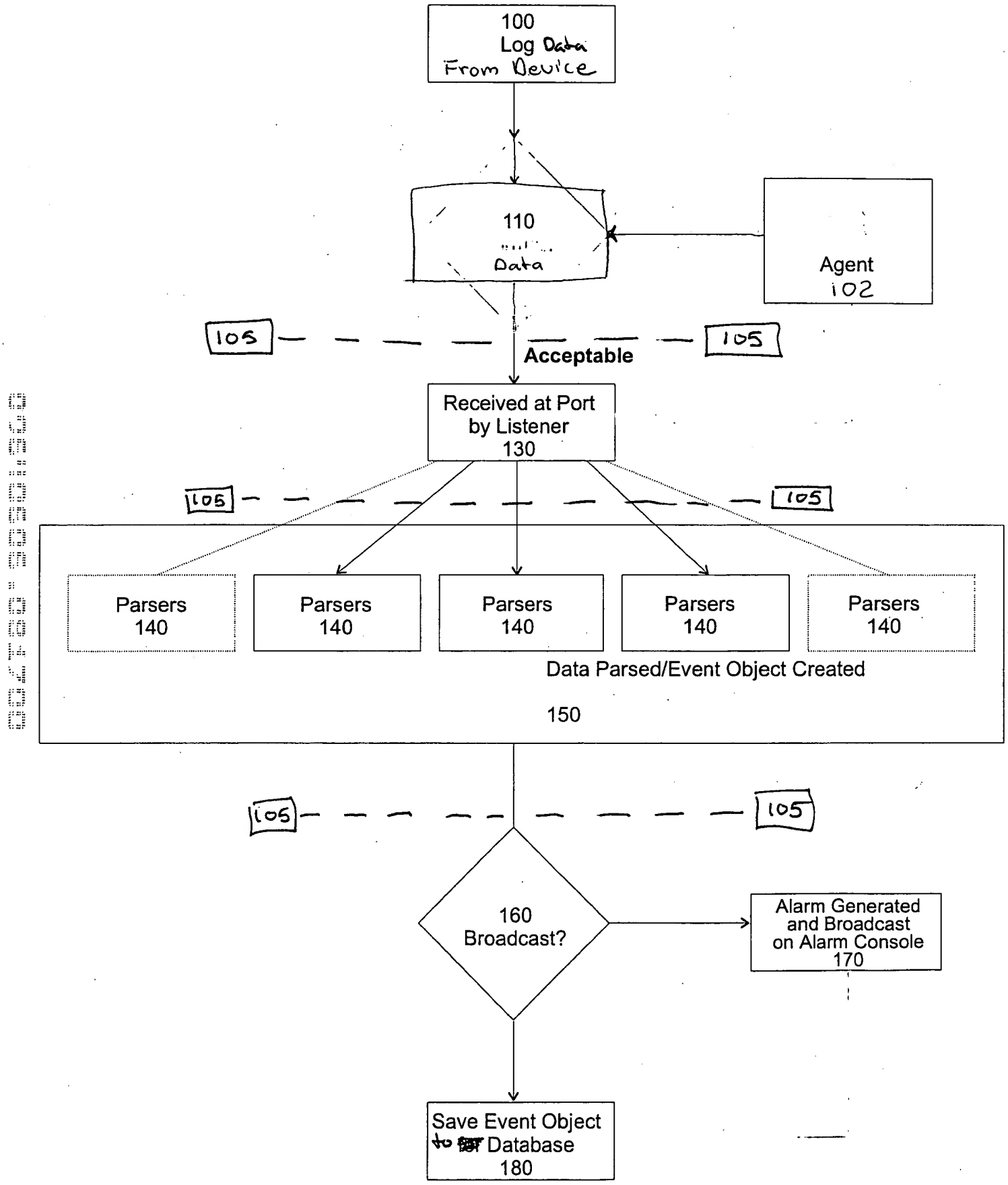

100
Log Data
From Device
110
Data
Agent
102
105
105
Acceptable
Received at Port
by Listener
130
105
105
Parsers
140
Parsers
140
Parsers
140
Parsers
140
Parsers
140
Data Parsed/Event Object Created
150
105
105
160
Broadcast?
Alarm Generated
and Broadcast
on Alarm Console
170
Save Event Object
to Database
180

Fig. 5

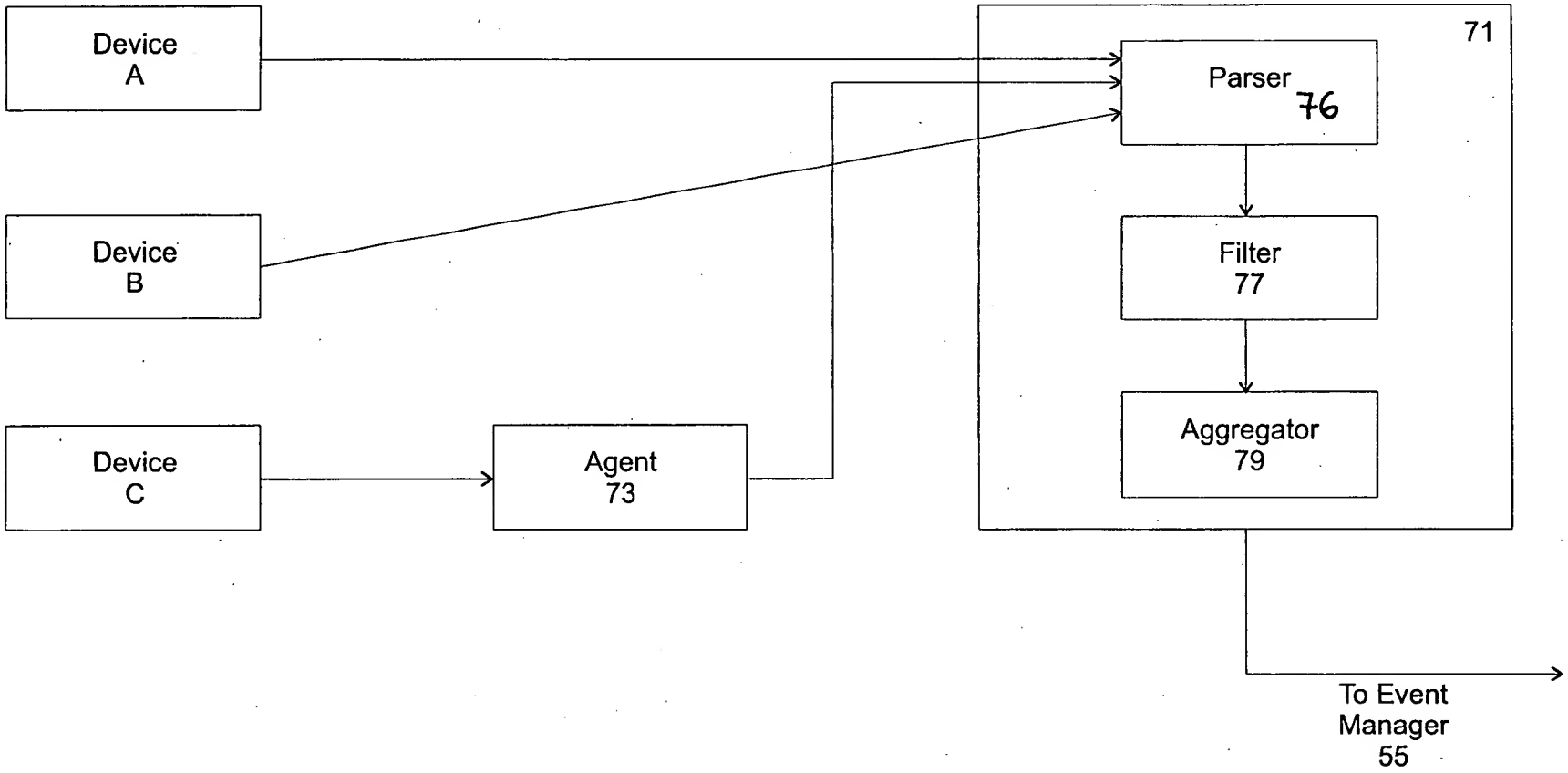

Device A
Device B
Device C
Agent 73
71
Parser 76
Filter 77
Aggregator 79
To Event Manager 55

Fig. 6

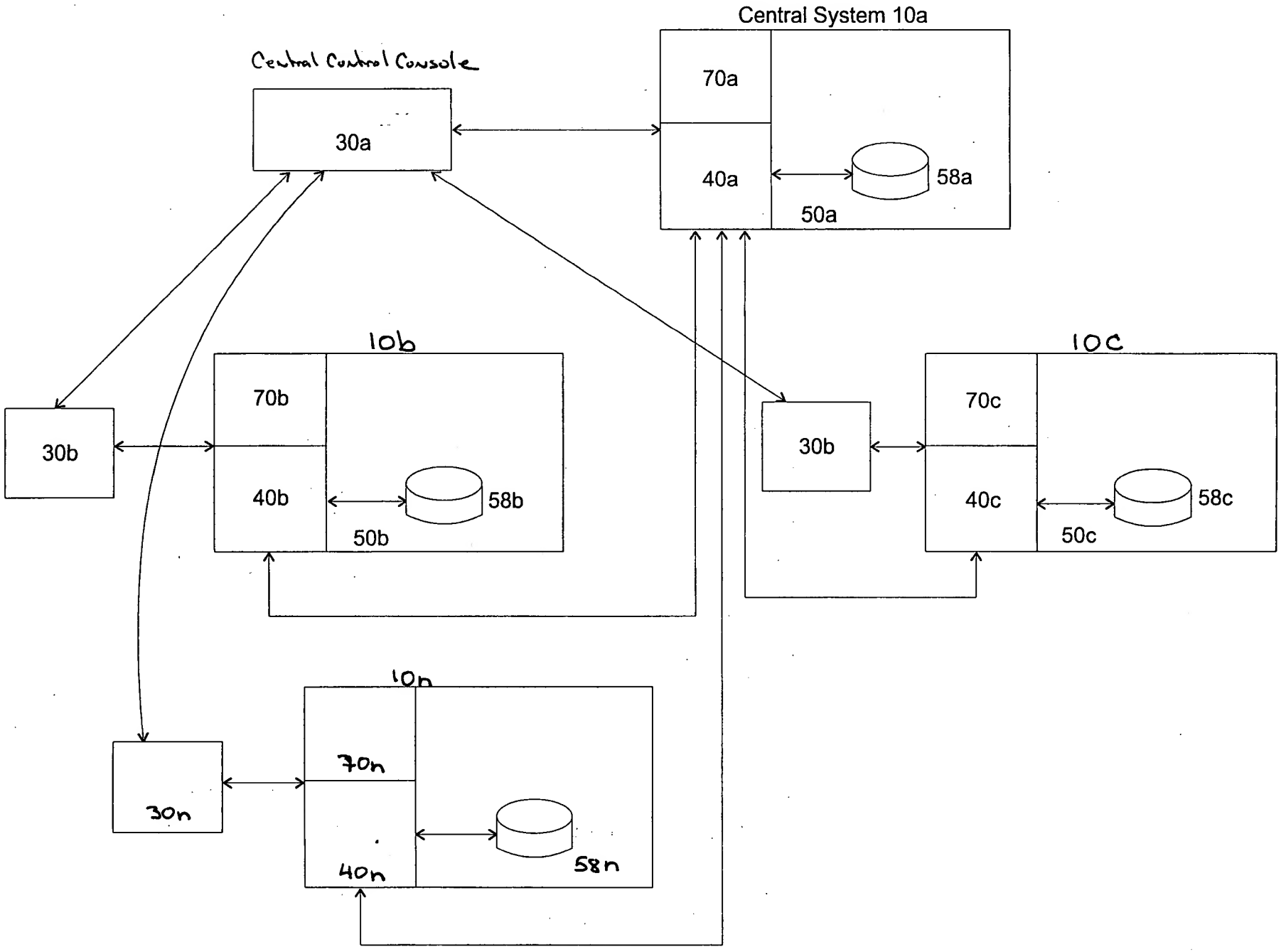
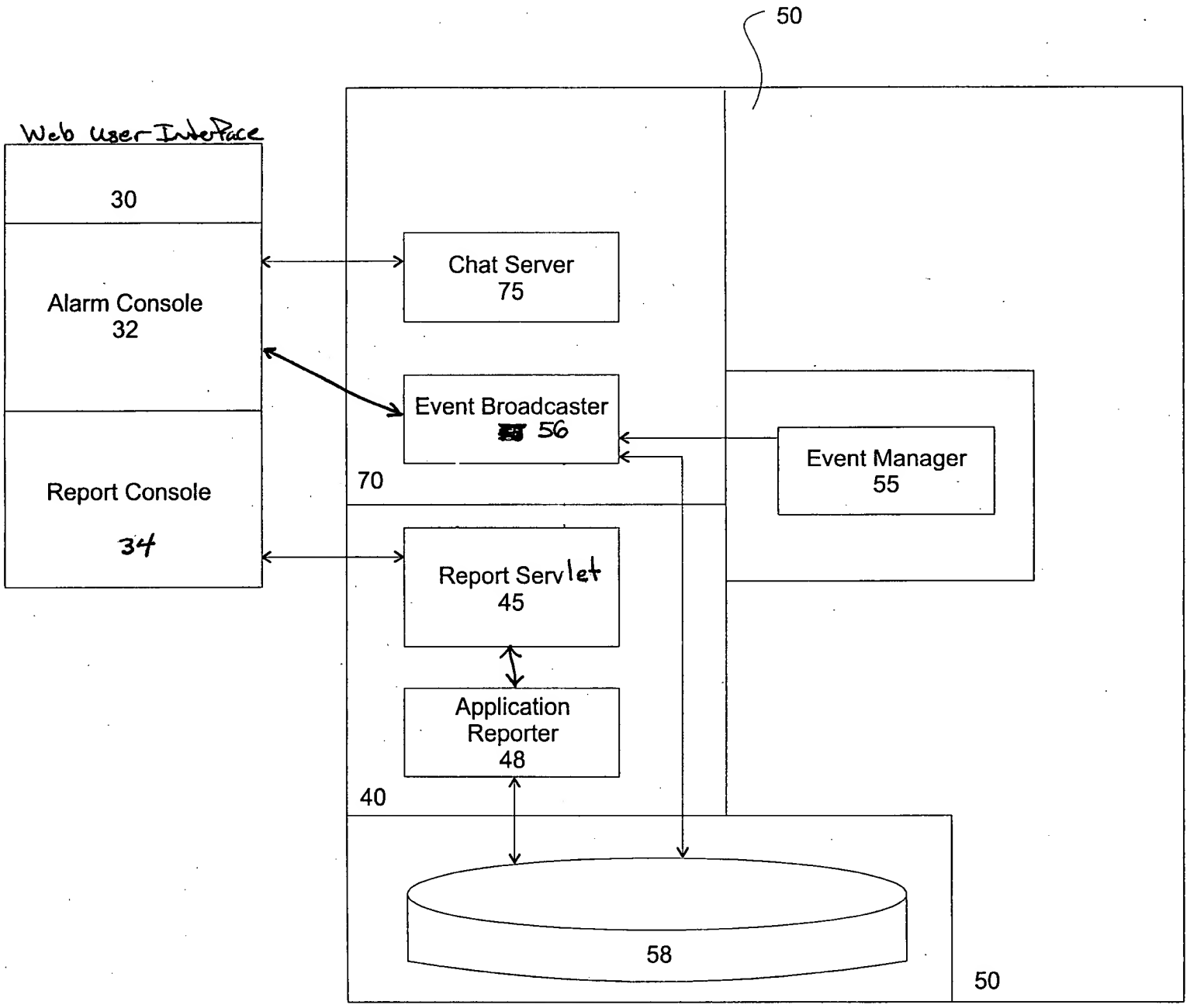

Central System 10a
Central Control Console
30a
70a
40a
58a
50a
10b
70b
30b
40b
58b
50b
10c
70c
30b
40c
58c
50c
10n
70n
30n
40n
58n

Fig. 7


50
Web User Interface
30
Alarm Console
32
Report Console
34
Chat Server
75
Event Broadcaster
56
70
Event Manager
55
Report Servlet
45
Application
Reporter
48
40
58
50

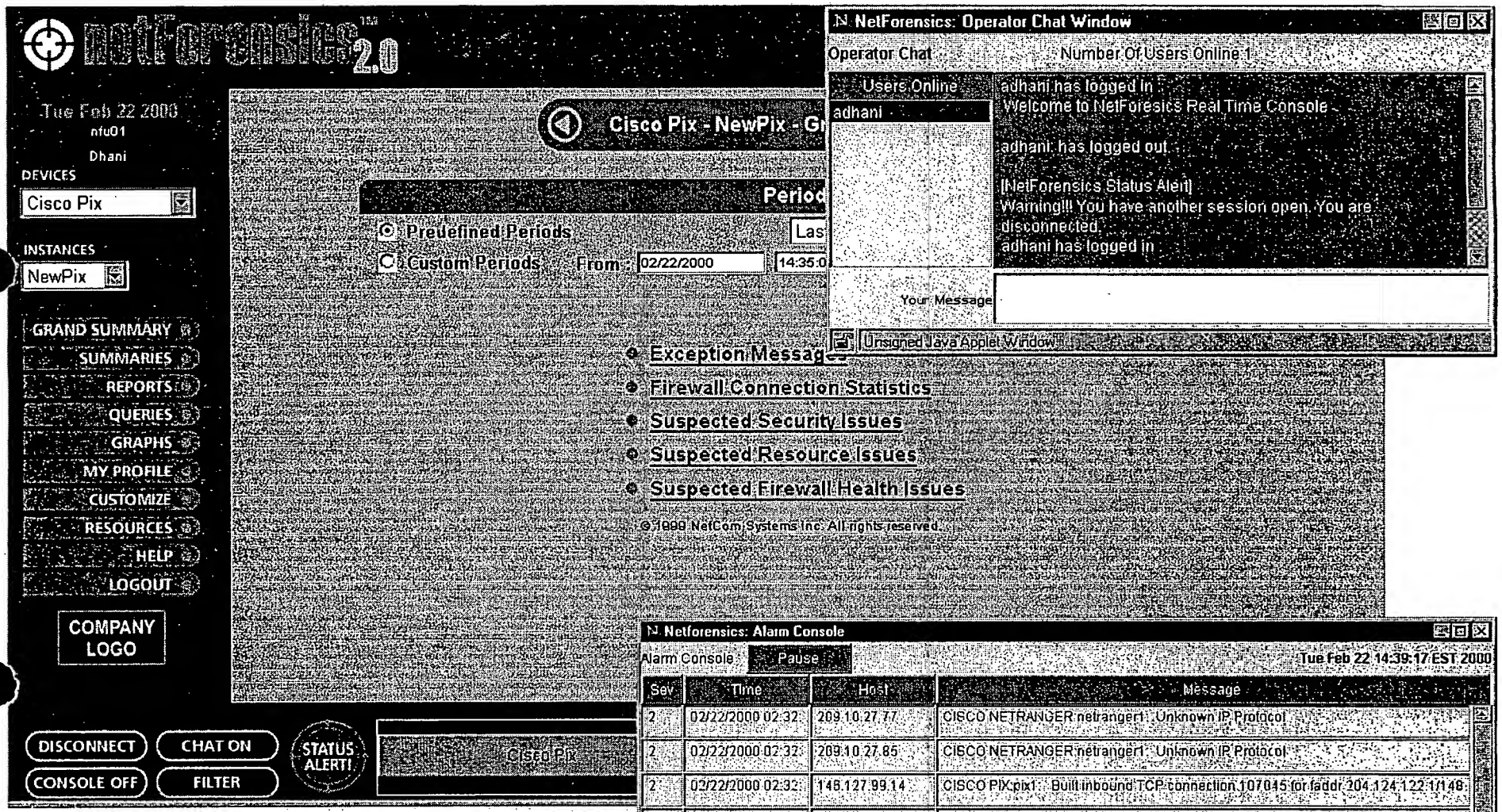

netforensics 2.0
Tue Feb 22 2000
nfu01
Dhani
DEVICES
Cisco Pix
INSTANCES
NewPix
GRAND SUMMARY
SUMMARIES
REPORTS
QUERIES
GRAPHS
MY PROFILE
CUSTOMIZE
RESOURCES
HELP
LOGOUT
COMPANY LOGO
DISCONNECT
CHAT ON
CONSOLE OFF
FILTER
STATUS ALERT!
Cisco Pix - NewPix - Gr
Period
Predefined Periods
Custom Periods
From :
02/22/2000
14:35:0
Exception Messages
Firewall Connection Statistics
Suspected Security Issues
Suspected Resource Issues
Suspected Firewall Health Issues
©1999 NetCom Systems Inc. All rights reserved.
NetForensics: Operator Chat Window
Operator Chat
Number Of Users Online 1
Users Online
adhani
adhani has logged in
Welcome to NetForesics Real Time Console
adhani has logged out
[NetForensics Status Alert]
Warning!!! You have another session open. You are disconnected.
adhani has logged in
Your Message
Unsigned Java Applet Window
Netforensics: Alarm Console
Alarm Console
Pause
Tue Feb 22 14:39:17 EST 2000
Sev
Time
Host
Message
2 02/22/2000 02:32 209.10.27.77 CISCO NETRANGER netrangerl Unknown IP Protocol
2 02/22/2000 02:32 209.10.27.85 CISCO NETRANGER netrangerl Unknown IP Protocol
2 02/22/2000 02:32 146.127.99.14 CISCO PIX pix1 Built inbound TCP connection 107045 for faddr 204.124.122.1/148
2 02/22/2000 02:32 209.10.27.77 CISCO NETRANGER netrangerl Unknown IP Protocol
1 02/22/2000 02:32 204.124.122.1 CISCO NETRANGER netrangerl TCP Ports
2 02/22/2000 02:32 161.15.96.96 CISCO PIX pix1 Deny TCP (no connection) from 161.15.96.96/2666 to 146.127.99.1
Unsigned Java Applet Window

Figure 8

Fig. 9

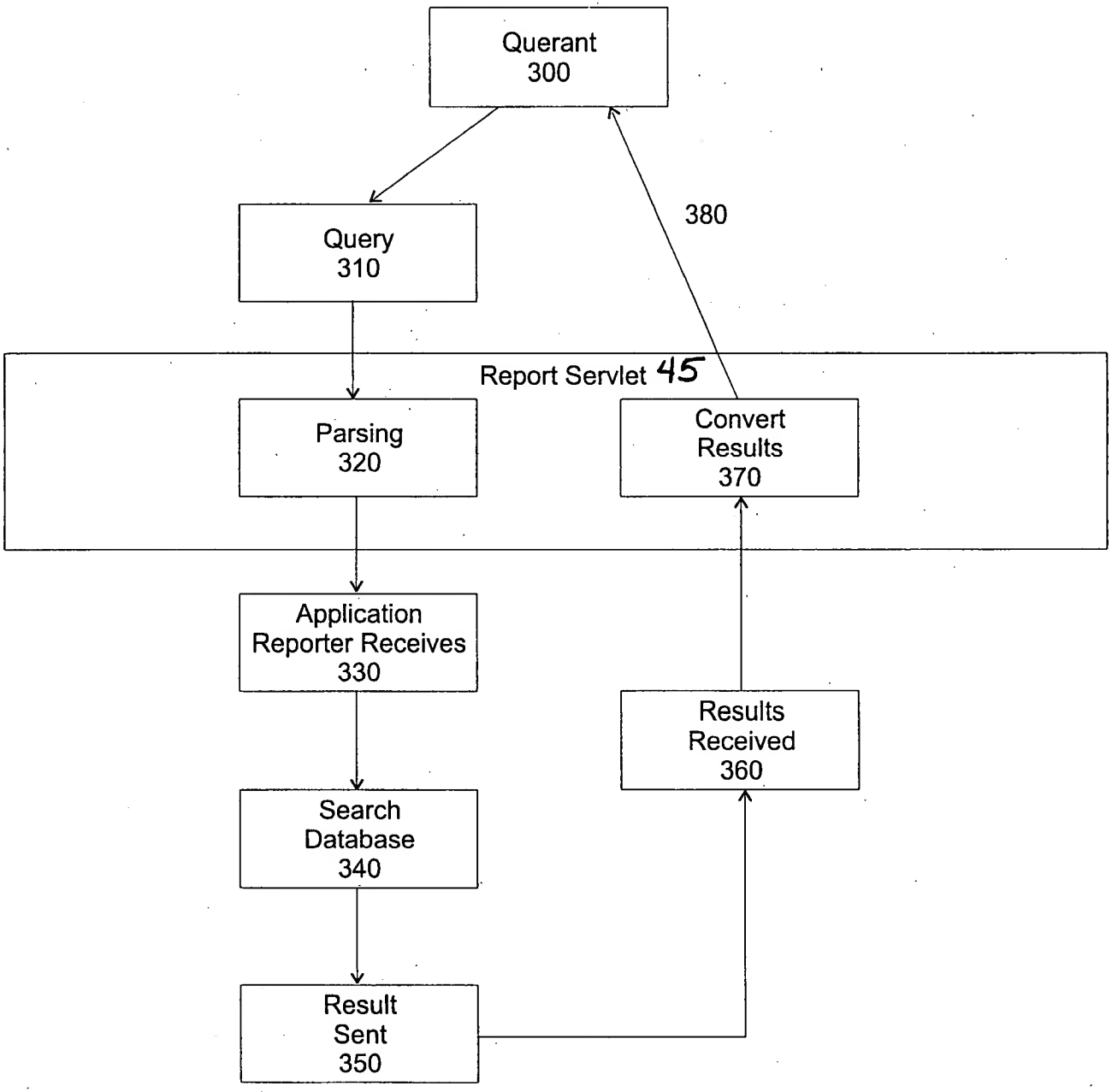

Querant
300
Query
310
380
Report Servlet 45
Parsing
320
Convert
Results
370
Application
Reporter Receives
330
Results
Received
360
Search
Database
340
Result
Sent
350

Fig. 10